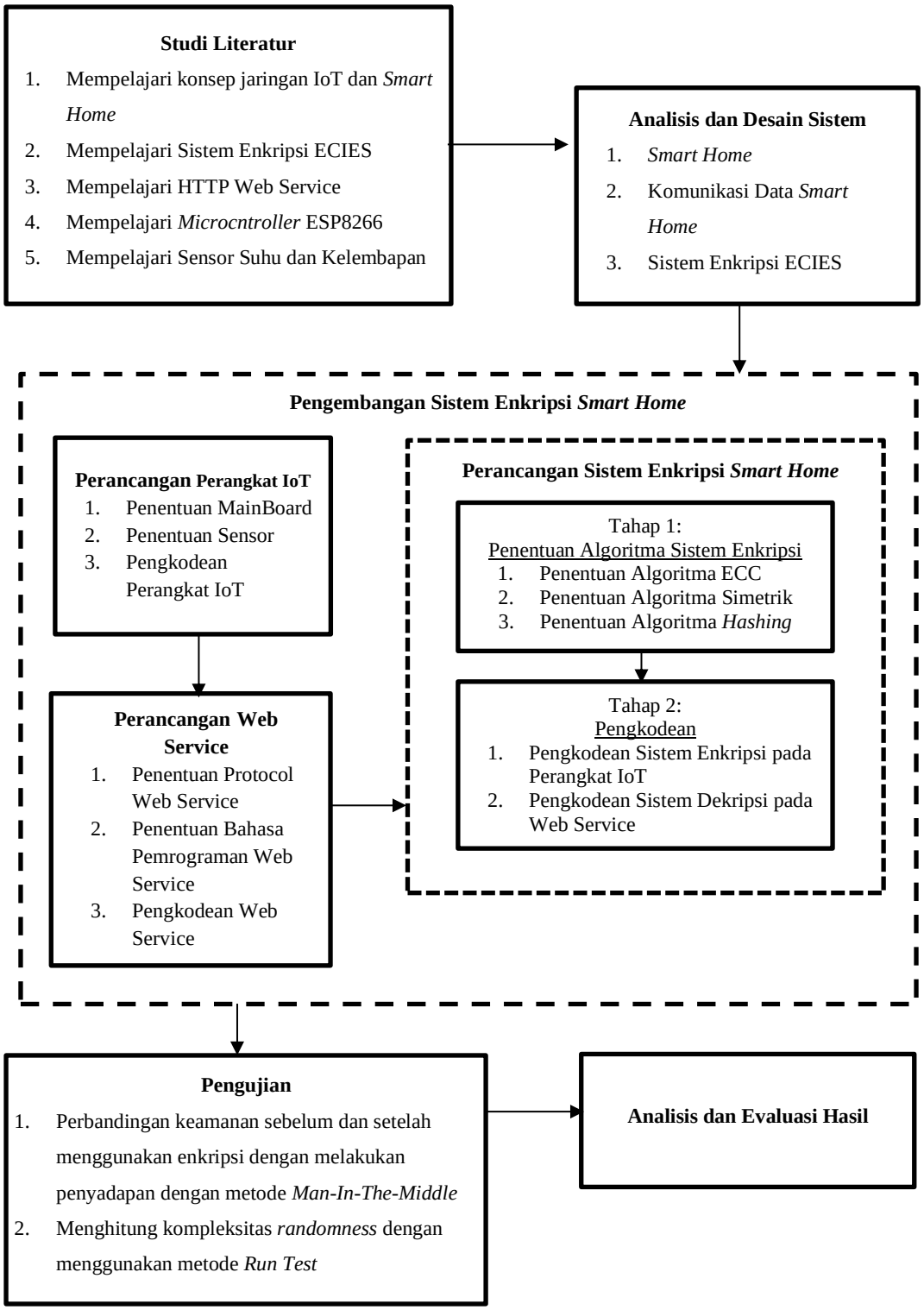
BAB III

METODE PENELITIAN

3.1 Desain Penelitian



Gambar 3.1 Desain Penelitian

3.1.1. Studi Literatur

Sebagai bahan referensi untuk penilitian, maka dilakukan studi literatur yang terkait dengan penelitian. Dari hasil studi literatur ini, penelitian menjadi lebih terstruktur untuk mengerjakan setiap tahap penelitian. Studi literatur ini meliputi:

1. *Smart Home*
2. Sistem Enkripsi ECIES
3. HTTP Web Service
4. Sensor Suhu dan Kelembapan

3.1.2. Analisis dan Desain Sistem

Merupakan tahap menganalisis hal-hal yang diperlukan dalam pelaksanaan proyek pembuatan sistem enkripsi *ECIES* pada *Smart Home*. Setelah melakukan analisis kemudian dilakukan penerjemahan dari data analisis kedalam bentuk gambar atau diagram yang mudah dimengerti yaitu infrastruktur sistem, detil algoritma dan alur program. Ini merupakan proses mempersiapkan suatu model sitem enkripsi sehingga dapat dilanjutkan pada tahap berikutnya.

3.1.3. Pengembangan Sistem Enkripsi *Smart Home*

Pengembangan sistem enkripsi *Smart* Home meliputi perancangan modul sensor, perancangan *Smart Home* dan perancangan sistem enkripsi ECIES dan juga tahap pengkodean sistem enkripsi pada perangkat IoT dan pengkodean sistem dekripsi pada web service.

3.1.3.1 Perancangan *Smart Home*

Perancangan *Smart Home* ini meliputi infrastruktur *smart home* dari mulai mengumpulkan data dari sensor kemudian di proses oleh *microcontroller* yang pada akhirnya data tersebut dikirimkan ke *server* melalui *gateway*.

3.1.3.2 Perancangan Perangkat IoT

Perancangan Modul Sensor ini meliputi rangkaian yang terdiri dari sensor dan *microcontroller*.

3.1.3.3 Perancangan Web Service

Perancangan web service ini meliputi alur pengiriman data dari perangkat IoT ke *server* dan perancangan database untuk penyimpanan data dari perangkat IoT.

3.1.3.4 Perancangan Sistem Enkripsi ECIES

Perancangan sistem enkripsi ECIES ini meliputi alur program enkripsi pada perangkat IoT dan alur program dekripsi pada *server*. Terdiri dari dua tahap yaitu penentuan algoritma dan pengkodean.

Pada tahap perancangan, akan ditentukan juga algoritma-algoritma yang akan digunakan untuk proses enkripsi, diantaranya yaitu:

1. Penentuan Algoritma ECC

   Algoritma ECC yang akan digunakan adalah ECC dengan kurva secp256k1. Algoritma ini digunakan untuk melakukan proses *Diffie-Hellman* untuk mendapatkan *private key*, *public key* dan *shared key*.

2. Penentuan Algoritma Simetrik

   Algoritma Simetrik yang digunakan adalah algoritma AES-128-CBC. Algoritma ini digunakan untuk melakukan enkripsi pesan yang menggunakan kunci berdasarkan algoritma ECC.

3. Penentuan Algoritma *Hashing*

   Algoritma *Hashing* yang akan digunakan adalah algoritma SHA-256. Algoritma ini digunakan untuk menghasilkan kunci MAC, kunci enkripsi dan HMAC yang berguna sebagai kode otentikasi pesan yang akan dikirimkan bersamaan dengan pesan yang telah terenkripsi.

Setelah algoritma yang akan digunakan telah ditentukan, maka selanjutnya dilakukan tahap pengkodean meliputi:

1. Pengkodean Sistem Enkripsi pada Modul Sensor
2. Pengkodean Sistem Dekripsi pada Web Service

3.1.4. Pengujian

Pada tahap ini, dilakukan pengujian terhadap sistem yang telah dibangun untuk menghasilkan data yang terenkripsi. Pengujian dilakukan

dengan memverifikasi bahwa data yang terenkripsi dapat diterima dan di dekripsi dengan baik sesuai dengan data yang belum di enkripsi pada *server*. Tahap uji coba ini meliputi pengujian perbandingan data sebelum dan sesudah diproses (enkripsi) oleh sistem, dan pengujian *randomness* untuk mengetahui tingkat keacakan kunci yang dihasilkan.

1. Enkripsi

   Pada tahap ini dilakukan pembandingan data yang telah dienkripsi dengan data yang belum dienkripsi dengan metode penyerangan *Man-In-The-Middle*

2. *Randomness*

   Pada tahap ini dilakukan untuk mengetahui tingkat keacakan sebuah kunci yang dihasilkan dari algoritma ECC menggunakan uji coba *Run Test*. Dengan persamaan sebagai berikut

$$p = \left(\frac{r - \left(\frac{2nm}{N} + 1\right)}{\sqrt{\frac{2nm(2nm - N)}{N^2(N-1)}}} \right)$$

   P = p-*statistic* yang akan dibandingan pada standar normal deviasi.

   r = jumlah *runs* pada seri.

   n dan *m* = frekuensi dari observasi dua kelas.

   N = total jumlah observasi (=n+m)

   Jika hasil nilai *p* adalah kurang dari 0.01, maka dapat disimpulkan panjang kunci yang dihasilkan oleh *random number generator* tidak *random*. Jika nilai *p* lebih dari 0.01 maka panjang kunci tersebut *random* (Rukhin et al., 2010).

3.1.5. Analisis dan Evaluasi Hasil

Setelah hasil data pengujian diperoleh, maka selanjutnya dilakukan proses analisis hasil. Analisis hasil ini meliputi perhitungan tingkat akurasi

dari program, apakah sesuai dengan yang diinginkan atau belum. Jika hasilnya masih belum memuaskan, maka dilakukan evaluasi untuk memperbaiki sistem agar menjadi lebih baik dan sesuai dengan yang diharapkan.

3.2 Alat dan Bahan Penelitian

3.2.1 Alat Penelitian

Alat penelitian yang digunakan sebagai berikut:

1.1 Perangkat Keras

a. Komputer
   1) *Processor* Intel Core I 5 4460 3.20 GHz
   2) RAM 16 GB
   3) *Hard Disk* 1 TB
   4) SSD 256GB

b. Perangkat IoT NodeMCU
   1) Clock Speed 80MHz/160MHz
   2) Flash 4Mbytes
   3) Digital I/O Pins 11
   4) Operating Voltage 3.3V
   5) Panjang 34.22mm
   6) Lebar 25.6mm
   7) Berat 3 gram

2.1 Perangkat Lunak

a. Arduino IDE

Arduino IDE ini digunakan sebagai alat untuk mengembangkan perangkat lunak dalam penelitian ini, dalam bahasa pemrograman C

b. Cain & Abel

Cain & Abel digunakan untuk melakukan *Sniffing*, *ARP spoofing*, dan *ARP poison routing*. Semua itu dilakukan untuk mendukung proses pengujian yang menggunakan teknik penyadapan.

c. Wireshark

Penggunaan wireshark ini adalah sebagai tools pendukung untuk membuktikan paket yang dikirimkan telah aman atau belum.

d. Cryptool

Penggunaan Cryptool ini sebagai *tools* pendukung untuk menganalisis data *randomness* yang di hasilkan oleh perangkat IoT.

3.2.2 Bahan Penelitian

Bahan penelitian yang digunakan berupa literature *textbook*, paper, tutorial, dan artikel yang didapat dari internet mengenai sistem enkripsi, *Smart Home*, kriptografi dan algoritma kriptografi ECC.